The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Rebecca J. Richards
Director of Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 703-235-0780

PIA@dhs.gov

Upon receipt, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSOnline and directly from the DHS Privacy Office via email: pia@dhs.gov, phone: 703-235-0780.

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

Please complete this form and send it to the DHS Privacy Office.
Upon receipt, the DHS Privacy Office will review this form
and may request additional information.

SUMMARY INFORMATION

DATE submitted for review: September 1, 2009

NAME of Project: Protected Criticial Infrastructure Information Management System (PCIIMS) Final Operating Capability (FOC)

Name of Component: National Protection and Programs Directorate

Name of Project Manager: Laura S. Kimberly

Email for Project Manager: laura.kimberly@dhs.gov

Phone number for Project Manager: 703.235.3010

TYPE of Project:

☒ **Information Technology and/or System***

☐ **A Notice of Proposed Rule Making or a Final Rule.**

☐ **Other: <Please describe the type of project including paper based Privacy Act system of records.>**

---

* The E-Government Act of 2002 defines these terms by reference to the definition sections of Titles 40 and 44 of the United States Code. The following is a summary of those definitions:

- "Information Technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. See 40 U.S.C. § 11101(6).
- "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

Note, for purposes of this form, there is no distinction made between national security systems or technologies/systems managed by contractors. All technologies/systems should be initially reviewed for potential privacy impact.

SPECIFIC QUESTIONS

1. Describe the project and its purpose:

The Protected Critical Infrastructure Information Management System (PCIIMS) Final Operating Capability (FOC) pulls together the capabilities of electronic PCII submission, submission validation, workflow, and protection, user management and oversight, training delivery, and metadata management. These capabilities are being enhanced to a final operating capability and consolidated from the current PCIIMS Initial Operating Capability (IOC) and Program Administrative Support System (PASS). The electronic submission, validation and management allow the PCII Program Office (PO) to easily streamline the electronic handling process for PCII data. The user oversight, management and training allow PCII accredited entities to perform oversight and auditing of their respective user communities.

The existing PIA on file was developed with the intent to cover the PCII Management System (PCIIMS), which included three primary capabilities; electronic submission, workflow management, and user management. Conceptually, these three capabilities all fell under the single system umbrella of PCIIMS. Briefly, these components provide the following capabilities;

--Electronic submission is a small online application that collects business contact information from submitters and receives data (attachments) for PCII consideration. Only the submitter's and facility POC's business contact information is collected.

--Workflow management is an internal PCII Office application for the processing, tracking, validation, marking, and storage of PCII data. This system simply processes and manages data from the electronic submission capability as well as PCII submission metadata from other sources- no additional data is collected.

--User management is a tool to assist the PCII Program Office and PCII Officers in the oversight and management of the PCII User Community. Users register with the system by providing basic business contact information about themselves and their work to allow the tool workflow to assign them to the appropriate oversight body and to deliver the appropriate PCII authorization materials. This workflow does not provide for any privilege assignment, all users are considered basic users (access to only their information) unless manually granted oversight ('PCII Officer) privileges by the PCII Program Office. Once users successfully complete the authorization process, which includes taking and passing a training course, they receive an authorized user number and a PCII training certificate of completion. These users can then handle PCII materials and verify other users through the tool through their authorized user number. The authorized user number allows users to enter it and the tool provides information back concerning the validity, expiration, and employer of the number holder. No additional information is revealed during the check. Users are

required to take PCII Training annually. The tool enforces this requirement by expiring a user's PCII Authorized User Certificate after one year as well as completely removing user accounts if training is not refreshed within 30 days of the certificate's expiration. The tool also facilitates reach back to authorized users for purposes of auditing and policy change notification as required by PCII Program policy.

Initially these three capabilities comprised the PCIIMS. However, due to development timelines and budget reporting issues the user management component of PCIIMS was pulled out and renamed the Program Administrative Support (PAS) System. The PAS System was then developed in parallel to PCIIMS to meet the user management requirement without further complicating the budget and reporting processes. During the recent Certification and Accreditation of the PAS System, the PCIIMS PIA was reviewed and deemed by the Privacy Office to cover the PCII user management capability under the new PAS System title.

Moving forward, the PCIIMS is being updated into the PCIIMS Final Operating Capability (FOC). This update does not require the collection of any new user information. The update is simply a refresh of the technologies, methodologies, and workflow used to deliver the original capabilities. Furthermore, because of changes to budget processes the three capabilities are being consolidated back into a single application. Since the current PCIIMS and PAS System fall under the original PCIIMS PIA, consolidating those capabilities into a single system aligns them back to the original intent of the documentation.

2. Status of Project:

☐ This is a new development effort.

☒ This is an existing project.

Date first developed: June 1, 2007

Date last updated: May 1, 2009

The original PCIIMS PIA was dated June, 2007. This PTA is a combination of the current PCIIMS. The user management functionality for PCIIMS (PASS) was incorporated in May, 2009. This PTA is for the PCIIMS FOC update, which combines all functionality developed to date into an integrated system.

3. Could the project relate in any way to an individual?[1]

[1] Projects can relate to individuals in a number of ways. For example, a project may include a camera for the purpose of watching a physical location. Individuals may walk past the camera and images of those individuals may be recorded. Projects could also relate to individuals in more subtle ways. For example, a

☐ No. Please skip ahead to the next question.

☒ Yes. Please provide a general description, below.

The system collects user (business contact) information as part of the PCII user management and oversight capability as well as during the electronic submission of PCII.

4. Do you collect, process, or retain information on: (Please check all that apply)

☒ DHS Employees

☒ Contractors working on behalf of DHS

☒ The Public

☐ The System does not contain any such information.

project that is focused on detecting radioactivity levels may be sensitive enough to detect whether an individual received chemotherapy.

5. Do you use or collect Social Security Numbers (SSNs)? (This includes truncated SSNs)

☒ No.

☐ Yes. Why does the program collect SSNs? Provide the function of the SSN and the legal authority to do so:

<Please provide the function of the SSN and the legal authority to do so.>

6. What information about individuals could be collected, generated or retained?

The system collects business contact information from users to allow for the delivery and management of training and user oversight. This includes providing individual's name, business name and address, business phone number and email, as well as a description of how they support homeland security. Additionally, the system manages PCII data submitted directly to the PCII Program Office. These submissions are accompanied by information from the submitter. This includes name, business name and address, business phone number and email, as well as similar business contact information for a facility/ infrastructure point of contact.

7. If this project is a technology/system, does it relate solely to infrastructure? [For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)]?

☒ No. Please continue to the next question.

☐ Yes. Is there a log kept of communication traffic?

☐ No. Please continue to the next question.

☐ Yes. What type of data is recorded in the log? (Please choose all that apply.)

☐ Header

☐ Payload Please describe the data that is logged.

<Please list the data elements in the log.>

8. Can the system be accessed remotely?

☐ No.

☒ Yes. When remote access is allowed, is the access accomplished by a virtual private network (VPN)?

☒ No.

☐ Yes.

9. Is Personally Identifiable Information[2] physically transported outside of the LAN? (This can include mobile devices, flash drives, laptops, etc.)

☒ No.

☐ Yes.

10. Does the system connect, receive, or share Personally Identifiable Information with any other DHS systems[3]?

☒ No

☐ Yes. Please list:

11. Are there regular (ie. periodic, recurring, etc.) data extractions from the system?

☐ No.

☒ Yes. Are these extractions included as part of the Certification and Accreditation[4]?

☒ Yes.

☐ No.

12. Is there a Certification & Accreditation record within OCIO's FISMA tracking system?

☐ Unknown.

☐ No.

☒ Yes. Please indicate the determinations for each of the following:

---

[2] Personally Identifiable Information is information that can identify a person. This includes; name, address, phone number, social security number, as well as health information or a physical description.

[3] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in TAFISMA.

[4] This could include the Standard Operation Procedures (SOP) or a Memorandum of Understanding (MOU)

Confidentiality:	☐ Low	☐ Moderate	☒ High	☐ Undefined
Integrity:	☐ Low	☐ Moderate	☒ High	☐ Undefined
Availability:	☐ Low	☒ Moderate	☐ High	☐ Undefined

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD REVIEW

(To be Completed by the DHS Privacy Office)

DATE reviewed by the DHS Privacy Office: September 19, 2009

NAME of the DHS Privacy Office Reviewer: Rebecca J. Richards

DESIGNATION

☐ **This is NOT a Privacy Sensitive System** – the system contains no Personally Identifiable Information.

☒ **This IS a Privacy Sensitive System**

Category of System

- ☒ IT System
- ☐ National Security System
- ☐ Legacy System
- ☐ HR System
- ☐ Rule
- ☐ Other:

Determination

- ☐ PTA sufficient at this time
- ☐ Privacy compliance documentation determination in progress
- ☐ PIA is not required at this time
- ☒ A PIA is required
  - ☒ System covered by existing PIA: PCII MS
  - ☐ A new PIA is required.
  - ☐ A PIA Update is required.
- ☐ A SORN is required
  - ☐ System covered by existing SORN:
  - ☐ A new SORN is required.

DHS PRIVACY OFFICE COMMENTS